OIPE JC100 JUN 08 2001 PATENT & TRADEMARK OFFICE

Attorney Docket: 439-972-011 June 6, 2001.

#20

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Patent Application of	
ROBERT H. SHELTON	BEFORE THE BOARD OF
Serial No. 09/025,279	PATENT APPEALS AND
Filed: February 17, 1997	INTERFERENCES
For: STANDING ORDER DATABASE SEARCH SYSTEM AND METHOD FOR INTRANET AND INTERNET APPLICATION	
GROUP ART UNIT: 2172	
EXAMINER: Jean B. FLEURANTIN	

RECEIVED JUN 13 2001 Technology Center 2600

APPEAL BRIEF FOR APPELLANT

HONORABLE COMMISSIONER OF PATENTS
AND TRADEMARKS
Washington, D. C. 20231

Sir:

This is a brief for an appeal from the rejection of all claims in the above-identified United States Patent Application.

REAL PARTY IN INTEREST

The instant application is assigned of record to Allcare Health Management System, Inc. whose address is 100 East 15th Street, Suite 620, Fort Worth, Texas 76102.

RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge and belief, there are

06/11/2001 HVUONG1 00000019 09025279
01 FC:120 310.00 OP

no related appeals or interferences.

STATUS OF CLAIMS

There are a total of 81 claims in the instant application, all of which were finally Rejected in the Office Action mailed November 21, 2000.

Claims 1-81 stand rejected under 35 USC 103(a)as being unpatentable over Evans United States Patent 5,924,074.

STATUS OF AMENDMENTS

The following amendments have been filed and entered in the application: 1. A Preliminary Amendment dated September 16, 1998;

2. An Amendment dated June 15, 1999 to which a response was made by Office Action mailed June 6, 2000;

3. A Citation of Prior Art that was mailed by Applicant on October 25, 1999; and

4. An Amendment dated September 5, 2000, to which a response was made finally rejecting the application by Office Action mailed November 21, 2000.

SUMMARY OF INVENTION

As set forth in Appellant's application, the present invention is directed to a system and method for individual

patients to protect the confidentiality of their medical records. To accomplish this, there is provided a medical data base supervisory control system having at least one data base including medical data individually relating to each of a plurality of patients, internet and/or intranet means including interconnected computers for requesting and accessing the medical data, means for identifying medical data for each of the patients with conditions required for accessing the medical data, such conditions including prior informed consent by the patient about whom such records pertain, and data processing means for comparing the request with conditions required for access of the data and, when the request fails to comply with the required conditions, for overtly denying access to the data.

To carry out the method according to the invention, there is disclosed a method of controlling access to medical data in a medical data base comprising maintaining at least one data base including medical data individually relating to each of a plurality of patients, identifying medical data for each of the patients with indicia indicative of conditions required for access to the medical data, selectively introducing requests for access to the data through an interconnected computer input terminal, comparing the requests with the required conditions for access, including in the required conditions the prior authorization by the patient about whom such records pertain;

and, when the requests fail to comply with the required conditions, automatically denying access to the data.

The system and method also embrace and integrate over internet and/or intranet connections access criteria that may be individualized for each patient or that may be identified with groups of patients.

Important to Appellant's invention is the intentional identification of each patient's record with individualized access criteria conditions that must be met if access that patient's record is not to be automatically denied. Thus, the broad aspects of the invention are characterized in the two independent claims (i.e., claims 1 and 42) which are set forth in Appendix A. Other aspects of the invention include within the conditions required for access, the prior informed consent by the person about whom the requested medical records pertain.

ISSUES

1. Whether the subject matters of Claims 1-81 are obvious and hence unpatentable within the meaning of 35 USC 103(a)over Evans United States Patent 5,924,074.

2. Whether provisions assertively permitting joint access by authorized health care providers is readable as "said conditions required for access of said data and, when said request fails to comply with said conditions, for denying access

to said data" (Examiner's assertion at the last three lines of Page 2 of the Office Action of November 21, 2000)(Emphasis added).

3. Whether a system that overtly or assertively denies access unless explicit access conditions are met is anticipated or rendered obvious by a tiered password system that affirmatively provides access when passwords are presented?

4. Whether "it would have been obvious to a person of ordinary skill in the art to have modified the teachings of Evans with the step of data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data and, when said request fails to comply with said conditions, for denying access to said data . . . ." (Examiner's assertion at lines 9-13 of page 3 of the Office Action of November 21, 2000).

5. Are relationships among patient data patentably indistinct from medical data individually relating to each of a plurality of patients? (Examiner's assertion at third and fourth lines from the bottom of page 4 of the Office Action of November 21, 2000).

6. What is meant by the term "substantial teaching" and where does it find authoritative support in rejecting claims? (Numerous assertions set forth in the Office Action of November 21, 2000, pages 6-10).

GROUPING OF CLAIMS

The claims on appeal are separately patentable and do not stand and fall together; and the reasons for the separate patentability are as follows.

It is noted that claims 1 and 42 are independent claims. Claim 1 is directed to a system and is the head claim for a number of dependent claims each defining a system combination believed patentably distinct from the others. Similarly, Claim 42 is directed to a method and is the head claim for a number of dependent claims each defining a method believed patentably distinct from the others.

THE REMAINING CLAIMS ARE ALL DEPENDENT CLAIMS AND ARE SEPARATELY PATENTABLE IN THAT THEY INCLUDE MEANS OR STEPS FURTHER DISTINGUISHING THEM FROM THE EVANS PATENT

Claims 2 and 43 define combinations that are patentably different from the combinations of Claims 1 and 42 respectively in that they further include a means or step for authenticating the identity of the requesting party.

Claims 3 and 44 further include a means or step to prevent access to information concerning medical records by any party without the prior authorization of the patient about whom such records pertain.

Claims 4 and 45 further include a means or step for tentatively identifying records fulfilling criteria specified in said request for medical data.

Claims 5 and 46 include elements of Claims 4 and 45 and additionally include a means or step for authenticating the identity of said patients.

Claims 6 and 47 include the elements of Claims 1 and 42 but additionally qualify the means or step for requesting said medical data in that they further include means or step for indicating what part of the records is desired.

Claims 7 and 48 include the elements of Claims 1 and 42 but additionally qualify the means or step for requesting access by stating that it includes a means or step for indicating the reason that said records are being requested.

Claims 8 and 49 also include the elements of Claims 1 and 42 but further include a means or step for identifying records fulfilling said request with data symbolic of patient identity.

Claims 9 and 50 are dependent to Claims 8 and 49 respectively, but further qualify the means or step for identifying records fulfilling said request by stating that they includes data symbolic of medical symptoms or reason for patient visit.

Claims 10 and 51 are also dependent to Claims 8 and 49 but further qualify the means for identifying records fulfilling said request by stating that it further includes data symbolic of types of diagnostic tests performed.

Claims 11 and 52 are dependent to Claims 10 and 51 but further include data symbolic of the attributes, levels or

findings indicated within the diagnostic tests.

Claims 12 and 53 are dependent to Claim 8 and 49 but further include data symbolic of modes of treatment or medical services rendered.

Claims 13 and 54 are dependent to Claims 8 and 49 but further include data symbolic of any ancillary services rendered.

Claims 14 and 55 are dependent to Claims 8 and 49 but further include data symbolic of attending physician identity.

Claims 15 and 56 also are dependent to Claims 8 and 49 but further includes data symbolic of date of care.

Claims 16 and 57 comprise the elements of Claims 1 and 42 but additionally include a particularizing characterization by indicating that the means for requesting and accessing the medical data include a means or step for indicating a "standing order" that will automatically initiate an attempt to retrieve certain predetermined types of medical data under specific pre-specified circumstances.

Claims 17 and 58 comprise the elements of Claims 1 and 42 but further describe the conditions required for accessing the medical data as including an indication of the names of each of the parties who's permission must be obtained prior to the release of the medical data.

Claims 18 and 59 are dependent on Claims 17 and 58 respectively, but further characterize the conditions required for accessing the medical data as including an indication of the

charge that will be assessed by the holder of the medical data for the part, or in the form, specified by the requesting party.

Claims 19 and 60 further characterize Claims 17 and 58 in stating that the conditions for accessing the medical data include indicating the time following receipt of all approvals that will be required for delivery of the medical data to the requesting party.

Claims 20 and 61 further qualify Claims 1 and 42 by stating that the data base includes a firewall limiting access to searching the data base solely to those who are authorized to do so.

Claims 21 and 62 further characterize the system of Claim 1 and method of Claim 42 by stating that there is included means for producing an indicia of the degree to which patient data match criteria specified in the request therefor.

Claims 22 and 63 extend the system of Claim 1 and method of Claim 42 to include means or step for a patient to grant permission for the release of his/her medical data.

Claims 23 and 64 extend the system of Claim 22 and method of Claim 63 to include billing means (or a step) having access to the medical data.

Claims 24 and 65 further qualify Claims 22 and 64 in that means or step for a patient to grant permission includes data symbolic of the identity of the patient and data symbolic of the preferred means for contacting the patient to request access to

and release of the patient's medical data.

Claims 25 and 66 further qualify the system of Claim 23 and method of Claim 64 in that they further characterize the means for a patient to grant permission as including data symbolic of rules to be followed in the event time elapses before such permission is granted in the case of predetermined types of requests for said medical data.

Claims 26 and 67 are a combination and method, respectively, of the elements of Claims 1 and 42 with means or a step for identifying the party requesting access to the medical data.

Claims 27 and 68 are a combination and method, respectively, of the system of Claim 26 and method of Claim 67 with a means or step for authenticating the identity of each party having right of approval for release of the medical data.

Claims 28 and 69 are a combination and method, respectively, of the system of Claim 27 and method of Claim 68 with a means or step for producing an indicia that all required approvals for release of the medical data have been secured.

Claims 29 and 70 are a combination and method, respectively, of the system of Claim 28 and method of Claim 69 with a means or step for producing an indicia of the required approvals for the release of the medical data that have not been secured or that have been specifically declined.

Claims 30 and 71 are a combination and method, respectively, of the system of Claim 20 and method of Claim 61 further

including data index means and an on-line memory cache.

Claims 31 and 72 are a combination and method respectively, of the system of Claim 30 and method of Claim 71 further including an interface engine enabling a search agent to index the data base of medical data.

Claims 32 and 73 are a combination and method, respectively, of the system of Claim 1 and method of Claim 42 further including means or step for billing the requesting party for a charge related to access to the medical data.

Claims 33 and 74 are a combination and method, respectively, of the system of Claim 1 and method of Claim 42 further including an online memory cache and means or step for delivering medical data to a requesting party including transmitting requested medical data held in digital form to the online memory cache.

Claims 34 and 75 are the system of Claim 33 or method of Claim 74 in which the online memory cache means includes a firewall limiting access to the memory cache exclusively to authorized users.

Claims 35 and 76 are the system of Claim 33 or method of Claim 74 further including a means or step for producing an indicia that the requested medical data have been received in the online memory cache means and are being held there for download by a requesting party.

Claims 36 and 77 are the system of Claim 34 or method of Claim 75 further including a means or step for the requesting

party to enter through the firewall and download the medical data.

Claims 37 and 78 are the system of Claim 1 or method of Claim 42 including a means or step for delivering medical data to a requesting party.

Claims 38 and 79 are the system of Claim 37 or method of Claim 78 further including a means or step for informing the requesting party when medical data is in a non-digital form together with the mode of available delivery.

Claims 39 and 80 are the system of Claim 1 or method of Claim 42 further including an encrypting means or step.

Claims 40 and 81 are the system of Claim 1 or method of Claim 42 further including a security log for retaining an audit trail with regard to communication within the system.

Claim 41 is the system of Claim 1 further including public portions and means for allowing parties to advertise in the public portions of the system.

It will thus be seen that each of Claims 1 to 41 defines a system and that each of Claims 42 to 81 defines a method that is patentably distinct from the others and that accordingly they do not rise or fall together.

ARGUMENT

I. THE APPEALED CLAIMS ARE PATENTABLE OVER EVANS PATENT 5,924,074

Introductory Preface: As will be observed from reference to the independent Claims 1 and 42, the claims under appeal define systems and methods characterized by having a data base including medical data individually relating to each of a plurality of patients. In order to avoid denial of access to such data, certain conditions must be met. These include informed consent (e.g., prior authorization) by the person whose medical data is being accessed.

1. The Evans Prior Art Reference:

Only one reference has been cited against the claims. This is United States Patent 5,924,074 granted to Jac A. Evans on July 13, 1999 and filed on September 27, 1996. As Evans states, his system automates and simplifies existing methods of patient chart creation, maintenance and retrieval. It creates and maintains all patient data electronically and thus can eliminate or supplement creating and maintaining physical data records. It furnishes healthcare providers with an intuitive, easy-to-use, icon-based interface that enables them to capture and analyze patient data quickly and efficiently. Healthcare providers enter patient data immediately at the point of care and this provides a complete audit trail for all patient data. In this manner, the

EMR (Electronic Medical Record) system disclosed in Evans transforms a patient chart from a static record of a few clinical interactions into a dynamic, real-time comprehensive record linked to an enterprise-wide clinical database.

The Evans system is also said to provide "instant access to patient's electronic medical record by authorized healthcare providers from any geographical location." (Column 14, lines 65-67). It enables complete replacement of physical records and permits healthcare providers such as physicians or nurse practitioners to electronically annotate patient's files and permits concurrent multiple access. It also envisions "patient confidentiality through a tiered password system." (Column 15, lines 21-22)

It will thus be observed that the thrust of the Evans reference is directed to providing Electronic Medical Records (EMR), thus making them more accessible and useful by authorized users; and that security considerations are incidental.

2. Discussion of Patentable Distinctions Over Evans:

Appellant has been unable to find any teaching or suggestion of the conditions required for access to patient data coupled with the overt denial of access as claimed by the claims on appeal. In the context of suggesting how his system facilitates patient record handling and access, Evans initially makes reference to general access by authorized entities. Subsequently,

he refers to tiered passwords for distinguishing between different entities so as to provide differing levels of access; and in that context, he states that "a patient may request restricted access to their data by only certain personnel." (Column 15, lines 29-31). Thus, while a type of restriction is envisioned, it is not a restriction within the purview of Appellant's claimed conditions as that term is properly interpreted when following the authoritative guidelines set forth below.

It is well known that while a claim is not limited to the details of the preferred embodiment set forth in the specification, claims are interpreted in light of the specification. Thus, in *Minnesota Mining & Manufacturing Co v. Johnson & Johnson Orthopaedics* 24 USPQ 2d 1321 (CAFC 1992) it is said "In defining the meaning of key terms in a claim, reference may be had to the specification, the prosecution history, prior art and other claims . . ." (Page 1327) Similarly, in *Renishaw PLC v Marposs Societa Per Azioni* 48 USPQ 2d 1117 (CAFC 1998) it is said: ". . . one may look to the written description to define a term already in a claim limitation, for a claim must be read in view of the specification of which it is a part." (Page 1120) (Underscoring added).

Now applying the foregoing principles to interpreting the meaning of the term "conditions" as set forth in Appellant's

claims, it will be recalled that in Appellant's specification, the conditions required to avoid denial of access include prior authorization by the patient about whom such record or records pertain. This can be provided either by an initial blanket approval, a prior approval for a limited number of people, or express approval by the patient for access by a party newly requesting access. In all instances there must be a prior approval by the patient before anyone can gain access to his records. That such is not taught by Evans was indicated in the Office Action of June 6, 2000 where, at page 3, it is said "...Evans does not specifically disclose a data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data and, when said request fails to comply with said conditions, for denying access to said data. However, Evans does disclose a method and system comprising the steps of organizing the patient data so as to form a patient record, and retrieving the patient record to access the patient data for use in the care of a patient, and obtaining a patient identifier, locating a patient record corresponding to the patient identifier (which is readable as data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data)" (citing column 3, lines 10-35 of the Evans patent). (Underscoring added).

Appellant has diligently studied the foregoing Examiner's

underscored quotation and is unable to find any basis for the assertion that it is "readable as data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data." On the contrary, the patient identifier appears merely to be a convenient tool to assist in locating a patient record and is irrelevant to the question of conditions required to avoid denial of access. Accordingly, it is believed that the Examiner's assertion is in error and should not be sustained.

Although the foregoing considerations are deemed to support patentability of Claims 1 and 41, additional support for their patentability is set forth in the following sections and, in particular, Section IV which deals with unobviousness and the fulfillment of a long felt need.

II. PROVISIONS ASSERTIVELY PERMITTING JOINT ACCESS BY AUTHORIZED HEALTH CARE PROVIDERS ARE NOT READABLE AS "SAID CONDITIONS REQUIRED FOR ACCESS OF SAID DATA

The second issue now addressed is whether provisions assertively permitting joint access by authorized health care providers is readable as "said conditions required for access of said data and, when said request fails to comply with said conditions, for denying access to said data" (Examiner's assertion at the last three lines of Page 2 of the Office Action of November 21, 2000)(Emphasis added). Appellant has diligently

attempted to find some basis for this assertion but has been unable to find any. How can a provision permitting access be interpreted as a condition for denying access? If there is a sustainable basis for such a conclusion, Appellant would appreciate being advised of same in the Examiner's reply brief. Otherwise, it is believed that such a conclusion is in error and should be overturned.

III. A SYSTEM THAT OVERTLY DENIES ACCESS UNLESS EXPLICIT ACCESS CONDITIONS, INCLUDING PRIOR PATIENT AUTHORIZATION, ARE MET IS NOT ANTICIPATED OR RENDERED OBVIOUS BY A TIERED PASSWORD SYSTEM THAT AFFIRMATIVELY PROVIDES ACCESS WHEN PASSWORDS ARE PRESENTED.

The third issue now addressed is: Whether a system that overtly or assertively denies access unless explicit access conditions, including prior patient authorization, are met anticipated or rendered obvious by a tiered password system that affirmatively provides access when passwords are presented? In addressing this issue, Appellant would show that there is no teaching or suggestion in the Evans reference (or in any other art of which Appellant is aware) that passwords as used by Evans are conditioned upon prior patient authorization. On the contrary, as Evans expresses, "through the use of a tiered password system . . the system provides several levels of security for access . . . For example, a system administrator may

have global password access to any patient data . . . whereas physicians may have access only to patient records within their specialty and nurses and staff may have access to only those patient records within their immediate care." Although Evans states that a patient may request restricted access to their data by only certain personnel, such is not correlated with the foregoing passwords. Accordingly, it is believed evident that the tiered password system as disclosed by Evans does not render obvious the conditions envisioned by Appellant, which conditions require prior affirmative authorization by the patient in order to avoid denial of access.

IV. IT WOULD NOT HAVE BEEN OBVIOUS TO A PERSON OF ORDINARY SKILL IN THE ART TO HAVE MODIFIED THE TEACHINGS OF EVANS WITH THE STEP OF DATA PROCESSING MEANS RESPONSIVE TO A REQUEST FOR PATIENT MEDICAL DATA FOR COMPARING SAID REQUEST WITH SAID CONDITIONS REQUIRED FOR ACCESS OF SAID DATA AND, WHEN SAID REQUEST FAILS TO COMPLY WITH SAID CONDITIONS, FOR DENYING ACCESS TO SAID DATA.

The Examiner asserted at lines 9-13 of page 3 of the Office Action of November 21, 2000 that "it would have been obvious to a person of ordinary skill in the art to have modified the teachings of Evans with the step of data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data and, when said request fails to comply with said conditions,

for denying access to said data . . . ." Another conclusion is also made in the last three lines of page 5 and the first three lines of page 6 of the Office Action of November 21, 2000 where it is said "It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have modified the teachings of Evans with the step when said request fails to comply with said conditions, for denying access to said data, because such modification would allow Evans to provide efficiently cost effective (sic) to move data instead of physical records and health care providers, and eliminates the mishandling loss, destruction of patient data typically associated with maintenance of physical data records." (citing col. 14, lines 30-41). (*The foregoing sentence does not seem to make sense but is quoted precisely as written in the Office Action. The parenthetical expression 'sic' is included to indicate that the quotation is precisely as written.*) In this connection, Appellant would respectfully ask how thus modifying Evans would then make it cost effective to move data? Evans already moves data. How could one legitimately visualize that modification of Evans to introduce impediments to moving data could in any way make it more cost effective? The contrary would appear to be true.

Thus, in response to the foregoing conclusions, Appellant avers that such conclusions by the Examiner are unsupported by any implicit or explicit suggestion of, or any real motivation

for, or the desirability of such modification, in the Evans patent itself or elsewhere. As such, the conclusions of "obviousness" made by the Examiner are nothing but unsupported opinion, and not proper basis for rejection. In this connection, it is Appellant's understanding that the Examiner is required to identify where the prior art provides a motivating suggestion for the modification as for example in the decision in *In re Jones,* 21 USPQ 2d 1941 (Federal Circuit, 1992) where the court held: "Before the PTO may combine the disclosures of two or more prior art references in order to establish *prima facie* obviousness, there must be some suggestion for doing so . . . *In re Fine,* 5 USPQ 2d 1596, 1598-99 (Fed Cir 1988)" [at 1943] (Emphasis Added). "The prior art must provide one of ordinary skill in the art the motivation to make the proposed molecular modifications needed to arrive at the claimed compound." [at 1944] (Emphasis added).

Moreover, the courts have advocated that even if the prior art may be modified as suggested by the Examiner, the modification is not obvious unless the prior art suggests the desirability for the modification as, for example, in the decision in *In re Fritch* 23 USPQ 2d 1780 (Fed Cir 1992), where the court held: "Mere fact that prior art may be modified to reflect features of claimed invention does not make modification, and hence claimed invention obvious unless desirability of such

modification is suggested by prior art . . ." [at 1780] (Emphasis Added).

As clearly stated by Judge Rich in *In re Soli* 137 USPQ 797, 801: "When, as in the instant case, the Patent Office finds, in the words of 35 U.S.C. 103, 'differences between the subject matter sought to be patented and the prior art,' it may not without some basis in logic or scientific principle, merely allege that such differences are either obvious or of no patentable significance and thereby force an appellant to prove conclusively that it is wrong." (Underscoring added).

Moreover, it is well settled that an Examiner's speculation or opinion is improper unless supported by **facts**. See *In re Lunsford* 148 USPQ721, 725 where it is said, "Moreover as a matter of law under 35 U.S.C.103, the examiner **must** substantiate his 'suspicions' on the basis of facts drawn from proper prior art. The issue to be resolved requires more than 'suspicions' it requires facts." and "it is not realistic . . . within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis added).

Appellant further calls attention to the criteria set forth by the Court of Appeals for the Federal Circuit in the case of *In*

re Rijckaert 28 USPQ 2d, 1955 (1993). There, the court stated: (1) "in rejecting claims under 35 U.S.C. 103, the Examiner bears the initial burden of presenting a prima facie case of obviousness. Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant"' (2) "when the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it **must** indicate where such a teaching or suggestion appears **in the reference**" (Emphasis added); (3) "The mere fact that a certain thing may result from a given set of circumstances is not sufficient . . ."

In further response to the foregoing, Appellant would respectfully show that, despite diligent search, he has been unable to find any teaching or suggestion (**implicit or explicit**) in either the Evans reference or any other art of which he is aware, of the automatic denial of access to a patient's record until a comparison of a request for a patient's record meets conditions a required for access thereto.

Moreover, in support of an assertion of unobviousness, Appellant would respectfully show that Appellant's claimed invention meets an important need long felt in the art, a compelling argument in support of patentability. As examples of such long felt and generally recognized need, Appellant presents the documents set forth in Items 1, 2 and 3 of Annex C to this

Brief. These documents are:

Item 1. *A Summary of References Which Demonstrate Both the Novelty and Demand for Allcare's Privacy Service*

Item 2. *Online Healthcare Gets Candid Assessment at Berkeley Summit*

Item 3. *Privacy Technology Still Missing the Mark*

In reviewing the foregoing Items, it is dramatically evident that some of the most inquiring and influential minds in the field of medical record privacy have given much attention and thought to the importance of maintaining patient privacy while providing for legitimate controlled access to their medical records yet without having achieved the *inspirational insight* manifest in Appellant's instant claims. While, in hindsight, such may seem more modest, it is well settled that although a "difference may have seemed slight (as has often been the case with some of history's great inventions, e.g., the telephone), [but] it may also have been the key to success and advancement in the art resulting from the invention." (*Jones et al v Hardy*, 220 USPQ 1021 CAFC 1984)(Underscoring Added). Appellant asserts that such is the case with the instant application.

In further support of unobviousness and consequent patentability of the instant claims, it has been observed authoritatively that "It is usually the application of old

principles to new methods or articles of manufacture that involved patentable subject matter." (*In re Watter* 64 USPQ 571 CCPA 1945, at page 573) Moreover, as Judge Learned Hand observed, "It is the obvious when discovered and put to use that most often proves invention." (*H. C. White Co v Morton E. Converse & Son Co.*, 2 Cir., 20 F. 2d 311, 313)

As the Examiner is undoubtedly aware "Evidence of secondary considerations may often be the most probative and cogent evidence in the record. It may <u>often establish that an invention appearing to have been obvious in light of the prior art was not</u>." (*Stratoflex Inc v Aeroquip Corp*, 218 USPQ 879, CAFC 1983) (Underscoring added). Since it is well known that satisfaction of a well known and long felt need is an important secondary consideration, Appellant believes it evident that the subjects defined by the independent Claims 1 and 42 are unobvious and patentable not only over the Evans reference but all other art of which Appellant is aware. Accordingly, it is respectfully requested that the rejection of Claims 1 and 42 be withdrawn.

V. <u>RELATIONSHIPS AMONG PATIENT DATA ARE PATENTABLY DISTINCT FROM MEDICAL DATA INDIVIDUALLY RELATING TO EACH OF A PLURALITY OF PATIENTS.</u>

Are <u>relationships</u> among patient data patentably indistinct from <u>medical data individually</u> relating to <u>each</u> of a plurality of

patients? Please see the Examiner's assertion at lines 4-5 of the penultimate paragraph on page 4 of the Office Action of November 21, 2000 where it is said " . . . relationships among the data [are] considered . . . readable as medical data individually relating to each of a plurality of patients (see, abstract, lines 1-17)" (Underscoring added). For convenience of reference, the only relevant reference Appellant has been able to find in the abstract appears at lines 10-12 thereof where it is said "The system likewise permits instant, sophisticated analysis of patient data to identify relationships among the data considered." (Underscoring added).

In response to the Examiner's allegation, Appellant would respectfully show that relationships are very different from the individual data itself. Thus, the distance from the earth to the sun may be more than 300 times the distance from the earth to the moon, but one cannot tell from such a relationship what the actual distances or other characteristics (individual data) are. Applying such to the situation at hand, relationships between patient data may be of little or no concern for privacy but the actual data for an individual patient may be extremely sensitive and require protection. Accordingly, it is deemed evident that the pronouncement made by the Examiner (and unsupported by definition, logic or reasoning) is in error and should not be upheld.

VI. WHAT IS THE PATENTABLE SIGNIFICANCE OF THE TERM "SUBSTANTIAL TEACHING" AND HOW SPECIFICALLY DOES IT RELATE TO UNOBVIOUSNESS AND PATENTABILITY OF APPELLANT'S CLAIMS

The Examiner repeatedly used the expression "Evans substantially teaches" in rejecting claims 2-40 (and corresponding method claims). Appellant is not aware of authority for rejections based on "substantial teaching". However, if that phrase is intended to mean that the subject matter of the claims is patentably unobvious thereover it is noted that claims 2-40 are all drawn in dependent form to Claim 1; and since it is evident from the observations set forth in Sections I, II, III, IV and V above that the subject matter of Claim 1 is unobvious over the Evans reference, it is not understood how the expression "substantially teaches" is applicable or is a valid basis for claim rejection.

Claim 41 was rejected on the following basis: "As per claim 41, Evans discloses a system as claimed, further comprises means for allowing parties to advertise in the public portions of said system (see, figure 22)." Is the Examiner saying that he is rejecting Claim 41 under the provisions of 35 USC 102? If so, that would appear to be in direct contradiction with his admission that such is not disclosed by Evans as was stated in the Office Action of June 6, 2000 where, at page 3, it is said "...Evans does not specifically disclose a data processing means responsive to a request for patient medical data for comparing

said request with said conditions required for access of said data and, when said request fails to comply with said conditions, for denying access to said data." (Underscoring added). If, on the other hand he is saying that the subject matter of Claim 41 is not unobvious over Evans, it is believed that such is in error for the reasons set forth above in connection with Claim 1 (to which Claim 41 is dependent).

The foregoing considerations have been presented specifically with respect to the system claims 1-41. However, since the method claims 42-81 correspond to the system claims 1-40, Appellant asserts these considerations support patentability of claims 42-81 as well.

As to the prior art, in Appellant's view and personal experience, the problems and failings of the present state-of-art in this area (specifically including systems such as disclosed in *Evans*) are illustrative of the material and unobvious differences between a system that functions with generalized access through passwords and a system such as that of Appellant which requires prior individual informed consent by each patient. Appellant's system affords the advantage of being fully able to operate in an extended area while providing each patient with the assurance that his or her medical records will not be made available to others without his or her informed consent. Thus, it fills a need long felt in the art and is unobvious and patentable thereover.

The remaining claims, i.e., Claims 2-41 and 43-81 are dependent to Claims 1 and 42 respectively and therefore are deemed to patentably distinguish over the prior art for the reasons set forth above in respect to Claims 1 and 42. They severally define sub-combinations which include additional elements and steps to further define over the art. These are discussed in the foregoing section relating to Grouping of Claims. However, attention is directed to particularly cogent examples defined by Claims 3 and 44 which emphasize the requirement for individual prior informed consent by patients whose records are involved before such record can be accessed. Further emphasis thereof is represented by Claims 24 and 65 which particularize on the preferred mode for contacting a patient to request approval for release of patient data. Accordingly, it is deemed evident that Claims 2-41 and 43-81 are unobvious over the art and should be allowed.

SUMMARY

By the Examiner's own statements, the *Evans* patent fails to disclose the subject matter of Appellant's claims as evidenced by the following quotation "...Evans does not specifically disclose a data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data and, when said request fails to comply with said conditions, for denying access to said data."

Moreover, for the reasons set forth above, the systems and methods defined by Appellant's claims are unobvious thereover. Hence, it is evident that the rejections made are in error, that the rejections should be reversed, and that the claims on appeal should be allowed.

Respectfully,

Andrew M. Hassell

Andrew M. Hassell
Registration No. 18182
Attorney for Appellant
12568 Burninglog Lane
Dallas, Texas 75243
Tel: (972) 234-6540
Fax: (972) 234-6540

CERTIFICATE OF MAILING

I hereby certify that the above-noted paper is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D. C. 20231, on June 6, 2001

Andrew M. Hassell

Andrew M. Hassell

OIPE JC100 JUN 08 2001 PATENT & TRADEMARK OFFICE

APPENDIX A

CLAIMS UNDER APPEAL

1. A medical data base supervisory control system comprising:

(a) at least one data base including medical data individually relating to each of a plurality of patients,

(b) means including interconnected computers for requesting and accessing said medical data,

(c) means for identifying medical data for each of said patients with conditions required for accessing said medical data, and

(d) data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access to said data and, when said request fails to comply with said conditions, for denying access to said data.

2. A system of Claim 1 further including means for authenticating the identity of the requesting party.

3. The system of Claim 2 further including means to prevent access to information concerning medical records by any party without the prior authorization of the patient about whom such records pertain.

4. The system of Claim 1 further including means for tentatively identifying records fulfilling criteria specified in said request for medical data.

5. The system of Claim 4 further including means for authenticating identity of said patients.

6. The system of Claim 1 wherein said means for requesting said medical data includes means for indicating what part of said records is desired.

7. The system of Claim 1 wherein said means for requesting access to said medical records includes means for indicating the reason said records are being requested.

8. The system of Claim 1 further including means for identifying records fulfilling said request with data symbolic of patient identity.

9. The system of Claim 8 wherein said means for identifying records fulfilling said request further include data symbolic of medical symptoms or reason for patient visit.

10. The system of Claim 8 wherein said means for identifying records fulfilling said request further include data symbolic of types of diagnostic tests performed.

11. The system of Claim 10 wherein said means for identifying records fulfilling said request further include data symbolic of the attributes, levels or findings indicated within said diagnostic tests.

12. The system of Claim 8 wherein said means for identifying records fulfilling said request further include data symbolic of modes of treatment or medical services rendered.

13. The system of Claim 8 wherein said means used for

identifying records fulfilling said request further include data symbolic of any ancillary services rendered.

14. The system of Claim 8 wherein said means used for identifying records fulfilling said request further include data symbolic of attending physician identity.

15. The system of Claim 8 wherein said means for identifying records fulfilling such request further include data symbolic of date of care.

16. The system of Claim 1 wherein said means for requesting and accessing said medical data includes means for indicating a "standing order" that will automatically initiate an attempt to retrieve certain predetermined types of medical data under specific pre-specified circumstances.

17. The system of Claim 1 wherein said conditions required for accessing said medical data includes an indication of the names of each of the parties who's permission must be obtained prior to the release of the medical data.

18. The system of Claim 17 wherein said conditions required for accessing said medical data further includes an indication of the charge that will be assessed by the holder of such medical data for the part, or in the form, specified by the requesting party.

19. The system of Claim 17 wherein said conditions for accessing said medical data includes means indicating the time

following the receipt of all approvals that will be required for the delivery of such medical data to the requesting party.

20. The system of Claim 1 wherein said at least one data base includes a firewall limiting access to searching such data base solely to those parties who are authorized to do so.

21. The system of Claim 1 wherein said means for identifying medical data fulfilling criteria specified in a request include means for producing an indicia of the degree to which patient data match said criteria specified in said request.

22. The system of Claim 1 including means for a patient to grant permission for the release of his/her medical data.

23. The system of Claim 22 wherein said at least one data base includes billing means having access to said medical data.

24. The system of Claim 22 wherein said means for a patient to grant permission includes data symbolic of the identity of said patient and data symbolic of the preferred means for contacting said patient to request access to and release of said patient's medical data.

25. The system of Claim 23 wherein said means for a patient to grant permission includes data symbolic of rules to be followed in the event time elapses before such permission is granted in the case of predetermined types of requests for said medical data.

26. The system of Claim 1 further including means for identifying the party requesting access to said medical data.

27. The system of Claim 26 further including means for authenticating the identity of each party having right of approval for release of said medical data.

28. The system of Claim 27 further including means for producing an indicia that all required approvals for the release of said medical data have been secured.

29. The system of Claim 28 further including means for producing an indicia of the required approvals for the release of said medical data that have not been secured or that have been specifically declined.

30. The system of Claim 20 further including data index means and on-line memory cache means for physically disconnecting said at least one data base from said data index means, online memory cache means and all other outside parties except during batch process of uploading pre-designated and fully-approved requests for medical data.

31. The system of Claim 30 further including interface engine means enabling a search agent means to index said at least one data base of medical data.

32. The system of Claim 1 further including means for billing said requesting party for a charge related to access to the medical data.

33. The system of Claim 1 further including online memory cache means and means for delivering medical data to a requesting party including means for transmitting requested medical data

held in digital form to said online memory cache means.

34. The system of Claim 33 wherein said online memory cache means includes a firewall limiting access to said memory cache means exclusively to authorized users.

35. The system of Claim 33 further including means for producing an indicia that said requested medical data have been received in said online memory cache means and are being held there for download by said requesting party.

36. The system of Claim 34 further including means for said requesting party to enter through said firewall and download said medical data from said memory cache means.

37. The system of Claim 1 including means for delivering medical data to a requesting party.

38. The system of Claim 37 further including means for informing said requesting party when medical data is in a non-digital form and the mode of available delivery.

39. The system of Claim 1 further including means for encrypting all communications within the system.

40. The system of Claim 1 further including security log means for retaining an audit trail with regard to all of the communications within said system.

41. The system of Claim 1 further including public portions, and comprising means for allowing parties to advertise in said public portions of said system

42. A method of controlling access to medical data in a

medical data base comprising:

(a) maintaining at least one data base including medical data individually relating to each of a plurality of patients,

(b) identifying medical data for each of said patients with indicia indicative of conditions required for access to said medical data,

(c) selectively introducing requests for access to said data through an interconnected computer input terminal,

(d) comparing said requests with said conditions; and, when said requests fail to comply with said conditions, automatically denying access to said data.

43. The method of Claim 42 further including a step of authenticating identities of parties making said requests.

44. The method of Claim 43 further includes the step of rejecting requests for information concerning medical records by any party without the prior authorization of the patient about whom such records pertain.

45. The method of Claim 42 further including the step of tentatively identifying records fulfilling criteria specified in said requests for medical data.

46. The method of Claim 45 further including a step of authenticating identities of said patients.

47. The method of Claim 42 further including steps of requesting said medical data and indicating what part of said data is desired by said requesting party.

48. The method of Claim 42 further including steps of requesting access to said medical records and indicating a reason said records are being requested.

49. The method of Claim 42 including a step of ensuring that records fulfilling said requests include data symbolic of patient identities.

50. The method of Claim 49 wherein said step of identifying records fulfilling said requests further include data symbolic of medical symptoms or reason for patient visit.

51. The method of Claim 49 wherein said step of identifying records fulfilling said requests further include data symbolic of types of diagnostic tests performed.

52. The method of Claim 51 wherein said step of identifying records fulfilling said requests further include data symbolic of the attributes, levels or findings indicated within said diagnostic tests.

53. The method of Claim 49 wherein said step of identifying records fulfilling said requests further include data symbolic of modes of treatment or medical services rendered.

54. The method of Claim 49 wherein said step of identifying records fulfilling said requests further include data symbolic of the ancillary services rendered.

55. The method of Claim 49 wherein said step of identifying records fulfilling said requests further include data symbolic of attending physician identity.

56. The method of Claim 49 wherein said step of identifying records fulfilling said requests further include data symbolic of date of care.

57. The method of Claim 42 wherein said step of selectively introducing requests for access to said medical data includes a step of indicating a "standing order" that will automatically initiate an attempt to retrieve certain predetermined types of medical data under specific pre-specified circumstances.

58. The method of Claim 42 wherein said conditions required for accessing said medical data include a step of indicating names of each party who's permission must be obtained prior to release of said medical data.

59. The method of Claim 58 wherein said conditions required for accessing said medical data include an indication of the charge that will be assessed by the holder of such medical data for the part, or in the form, specified by the requesting party.

60. The method of Claim 58 wherein said conditions for accessing said medical data include a step of indicating the time following the receipt of all approvals that will be required for the delivery of such medical data to the requesting party.

61. The method of Claim 42 wherein maintaining said at least one data base includes maintaining a firewall limiting access to searching said data base solely to those parties who are authorized to do so.

62. The method of Claim 42 further including providing a

data index, and wherein identifying medical data fulfilling criteria specified in a request includes a step of producing an indicia of the degree to which data listed in said data index match said criteria specified in said request.

63. The method of Claim 42 including a step of providing for a patient to grant permission to release of such medical data.

64. The method of Claim 63 wherein said step of identifying medical data includes a step of billing for access to said medical data.

65. The method of Claim 63 wherein said step of providing for a patient to grant permission includes data symbolic of the identity of said patient and data symbolic of a preferred means for contacting said patient to request access to and to release of said patient's medical data.

66. The method of Claim 64 wherein said step of providing for a patient to grant permission includes providing data symbolic of rules to be followed in the event time elapses before said permission is granted in the case of pre-determined types of requests for said medical data.

67. The method of Claim 42 further including a step of identifying a party requesting access to said medical data.

68. The method of Claim 67 further including a step of authenticating identity of each party with a right of approval to release of said medical data.

69. The method of Claim 68 further including a step of

producing an indicia that all required approvals for release of said medical data have been secured.

70. The method of Claim 69 further including a step of producing an indicia of approvals required for release of said medical data that have not been secured, or that have been specifically declined.

71. The method of Claim 61 further including steps of providing a data index and online memory cache, and physically disconnecting said at least one data base from said data index, said online memory cache and all other outside parties except during batch process of uploading pre-designated and fully-approved requests for medical data.

72. The method of Claim 71 further including a step of providing an interface engine for search agent means to index said at least one data base of medical data.

73. The method of Claim 42 further including a step of billing a requesting party for a charge related to delivery of medical data.

74. The method of Claim 42 further including steps of providing an online memory cache and delivering medical data to a requesting party and transmitting records in digital form to said online memory cache.

75. The method of Claim 74 further including providing a firewall limiting access to said memory cache exclusively to authorized users.

76. The method of Claim 74 further including a step of producing an indicia that requested medical data have been received in said online memory cache and are being held there for download by a requesting party.

77. The method of Claim 75 further including a step of permitting a properly credentialed requesting party to enter through said firewall and download said medical data from said memory cache.

78. The method of Claim 42 including a step of delivering records to the requesting party.

79. The method of Claim 78 further including a step of informing a requesting party when medical data is in a non-digital form and the mode of such delivery.

80. The method of Claim 42 further including a step of encrypting selected communications within said system.

81. The method of Claim 42 further including a step of creating a security log and retaining an audit trail with regard to all of the communications between parties using said system.

APPENDIX B

AUTHORITIES ON WHICH RELIED

Appellant relies upon the following authorities:

1. In re Fritch 23 USPQ 2d 1780 (CAFC, 1992) "The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification. . . . It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." (Page 1783)

2. Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Company 221 USPQ 481 (CAFC, 1984). "The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness of making the combination. (At page 488)

3. In re Lunsford 148 USPQ 721, 725 "Moreover as a matter of law under 35 U.S.C.103, the examiner **must** substantiate his 'suspicions' on the basis of facts drawn from proper prior art. The issue to be resolved requires more than 'suspicions' it requires facts." and "it is not realistic . . . within the

framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis added).

4. In re Rijckaert 28 USPQ 2d, 1955 (CAFC, 1993) " . . in rejecting claims under 35 U.S.C. 103, the Examiner bears the initial burden of presenting a prima facie case of obviousness. Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant" . . "when the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it **must** indicate where such a teaching or suggestion appears **in the reference**" (Emphasis added) . . . "The mere fact that a certain thing may result from a given set of circumstances is not sufficient . . ."

5. In re Soli 137 USPQ 797, 801 (passage is recited above in text of arguments) "When, as in the instant case, the Patent Office finds, in the words of 35 U.S.C. 103, 'differences between the subject matter sought to be patented and the prior art,' it may not without some basis in logic or scientific principle, merely allege that such differences are either obvious or of no patentable significance and thereby force an appellant to prove conclusively that it is wrong." (Underscoring added).

6. Minnesota Mining & Manufacturing Co v. Johnson & Johnson Orthopaedics 24 USPQ 2d 1321 (CAFC, 1992) "In defining

the meaning of key terms in a claim, reference may be had to the specification, the prosecution history, prior art and other claims . . ."(Page 1327)

7. Renishaw PLC v Marposs Societa Per Azioni 48 USPQ 2d 1117 (CAFC, 1998) " . . . one may look to the written description to define a term already in a claim limitation, for a claim must be read in view of the specification of which it is a part." (Page 1120).

8. In re Jones, 21 USPQ 2d 1941 (CAFC, 1992) "Before the PTO may combine the disclosures of two or more prior art references in order to establish *prima facie* obviousness, there must be some suggestion for doing so . . . *In re Fine*, 5 USPQ 2d 1596, 1598-99 (Fed Cir 1988)" [at 1943]. The prior art must provide one of ordinary skill in the art the motivation to make the proposed molecular modifications needed to arrive at the claimed compound." [at 1944] (Emphasis added).

9. In re Fine, 5 USPQ 2d 1596, 1598-99 (CAFC, 1988) Please see the quotation under In re Jones immediately above.

10. Jones et al v Hardy, 220 USPQ 1021 (CAFC, 1984) ". . . difference may have seemed slight (as has often been the case with some of history's great inventions, e.g., the telephone), [but] it may also have been the key to success and advancement in the art resulting from the invention." (Emphasis added).

11. In re Watter 64 USPQ 571 (CCPA, 1945) at page

573 "It is usually the application of old principles to new methods or articles of manufacture that involved patentable subject matter."

12. H. C. White Co v Morton E. Converse & Son Co., 2 Cir., 20 F. 2d 311, 313. Judge Learned Hand observes: "It is the obvious when discovered and put to use that most often proves invention."

13. Stratoflex Inc v Aeroquip Corp, 218 USPQ 879, (CAFC 1983) "Evidence of secondary considerations may often be the most probative and cogent evidence in the record. It may often establish that an invention appearing to have been obvious in light of the prior art was not."

APPENDIX C

ARTICLES EVIDENCING LONG FELT UNMET NEED

Item 1: *A Summary of References Which Demonstrate Both the Novelty and Demand for Allcare's Privacy Service*

Item 2: *Online Healthcare Gets Candid Assessment at Berkeley Summit*

Item 3: *Privacy Technology Still Missing the Mark*

Comment: In reviewing the foregoing Items, it is dramatically evident that many of the most inquiring and influential minds have given much attention and thought to the importance of maintaining patient privacy while providing for legitimate controlled access to their medical records yet without having achieved the *inspirational insight* manifest in Appellant's claimed subjects. (Important felt need not previously met)

OIPE JC189
JUN 0 8 2001
PATENT & TRADEMARK OFFICE

APPENDIX C

ARTICLES EVIDENCING LONG FELT UNMET NEED

ITEM 1

A SUMMARY OF REFERENCES WITH DEMONSTRATE BOTH THE NOVELTY AND DEMAND FOR ALLCARE'S PRIVACY SERVICE

OIPE JC189 JUN 0 8 2001 PATENT & TRADEMARK OFFICE

PRIVACY APPLICATION

A SUMMARY OF REFERENCES WHICH DEMONSTRATE BOTH THE NOVELTY AND DEMAND FOR ALLCARE'S PRIVACY SERVICE

Allcare™ Health Management System, Inc. has filed a patent application on a database search facility that contains a number of unique elements, including the ability to efficiently share patient records among authorized persons and simultaneously allow for informed consent to assure that individual pricacy considerations are addressed.

The following quotes and referenced documents, which were gathered contemporanously with the filing of the patent application evidence the novelty of the approach as well as the propsective widespread demand for the service.

The San Jose Mercury News, a widely recognized online resource for Silicon Valley companies reported the following headline in its March 4, 1997 Morning edition: "The electronic privacy issue is shaping up as a major-league battle in the 105th Congress, where more than a dozen new bills have been introduced this session. On the eve of the annual *Computers, Freedom & Privacy conference* March 11-14 in Burlingame, *Salon magazine* talks with Marc Rotenberg, co-founder of the *Electronic Privacy Information Center*, about the political climate enveloping the issue."

Wired Magazine covered the issue from a different angle in a March 5, 1997 story entitled *Panel Urges Medical Data Protection*, which noted: "Right now, if your medical records are on a computerized database or are transmitted, you run the risk of having them seen by people you never dreamed would be perusing your health information." The story also references a National Research Foundation *advisory panel report* funded by the National Library of Medicine, the Warren Grant Magnuson Clinical Center of the National Institutes of Health, and the Massachusetts Health Data Consortium which urges "industry standards, regulatory action, and pressure from consumers . . . to bolster the privacy and security of electronic patient records."

These resources, together with the written and oral testimony before various Congressional committees and other sources describe the state of the technology and law at the time Mr. Shelton's system and method patent application was filed. The following sections present highlights from the subcommittee hearings with regard to *H.R. 52. Fair Health Information Practices Act of 1997*, a bill introduced by *Rep. Condit* (D-CA) on January 7, 1997, to establish a code of fair information practices for health information, to amend section 552a of title 5, United States Code, and for other purposes.

FROM TESTIMONY BEFORETHE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, SUBCOMMITTEE ON PRIVACY AND CONFIDENTIALITY
(January 13-14, 1997)

In his opening remarks, Dr. Robert Gellman, a privacy and information policy consultant in Washington and the subcommittee chair stated: "We intend to cover the full range of fair information practices issues, including patient's rights, limits on use and disclosure of information, health identification numbers, pre-emption of state laws and privacy-enhancing technologies when available, sometimes known as PETs -- privacy-enhancing technologies."

The subcommittee's first witness was Dr. David Korn, Professor of Pathology, and immediate past Vice President of Stanford University, Dean of the Stanford Medical School and a distinguished scholar in residence at the AAMC. *Dr. Korn's testimony* provides an excellent summary of the witnesses who testified during the two days. He stated: "The difficult challenge before this committee is to find a point of balance that will enable to us to enhance the security of confidential medical information and reduce the probability of its misuse, without substantially impairing the access and communication that are essential to the effective delivery of medical care, the efficient functioning of the health care delivery system and the pace of biomedical and health services research.

"But given the requirements for access and communication in the real worlds of medical care and biomedical research, *such levels of security in my judgment are fanciful*. More realistic would be to develop the best security mechanisms feasible from a cost benefit perspective, and couple that effort with effective measures to prohibit the discriminatory misuse of such information by employers, insurance companies or others.

"Unfortunately, we as a society have not succeeded in reaching that objective. In the absence of such effective measures, much effort is directed toward restricting the creation and accessibility of information, and building firewalls to insure its confidentiality."

Dr. Elizabeth Andrews, Chairperson for the Committee on Data Privacy of the International Society for Pharmacoepidemiology (ISPE), the director of epidemiology for Glaxo Wellcome and an adjunct associate professor of epidemiology at the University of North Carolina School of Public Health, stated: "Our studies often require data from files years after the medical events in question, years after patients have left a particular health plan, and sometimes after patients have died. *Requiring authorization for each research use is simply not feasible*."

FROM TESTIMONY BEFORETHE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, SUBCOMMITTEE ON PRIVACY AND CONFIDENTIALITY
(February 3-4, 1997)

On February 3, 1997, David L. Larsen, Director of Health Care Services at Salt Lake City-based Intermountain Health Care (IHC), testifyied on behalf of the American

Association of Health Plans (AAHP) which represents 1,000 HMOs, PPOs, and similar network plans providing care to over 120 million Americans. *In his testimony, Mr. Larsen stated*: "AAHP supports this Committee's efforts to protect against the unauthorized and inappropriate use of patient information while at the same time facilitate the coordination and delivery of high quality, network-based health care. It is important that your recommendations recognize the special needs of integrated delivery systems.

"In order to manage and improve the health outcomes of the population we insure, we must be able to share information among IHC corporate entities -- our physicians, hospitals, and health plans. IHC has developed electronic medical records and common databases to facilitate this communication. Preventing the creation of these common databases, limiting the type of data which can be shared within the IHC integrated delivery system, or *requiring a patient's authorization for each and every transaction and transfer of data*, would severely limit IHC's ability to measure and improve the health outcomes of our enrollees."

Also on February 3, Jeanne Scott, Director of Government and Legal Affairs for Oklahoma-based CIS Technologies, Inc., a subsidiary of National Data Corporation (NDC), testified on behalf of the Association for Electronic Health Care Transactions (AFEHCT), a trade organization who's member companies process over 2 billion electronic transactions annually. *In her testimony, Ms. Scott said*: "CIS and NDC support workable systems that will OPTIMIZE individual protections and assure that the advantages offered by the EDI and electronic commerce in health care will not be outweighed by the costs to individual privacy and personal freedom."

She later clarified: "But OPTIMIZATION does not mean maximization . . . . We cannot allow such an important issue [as reducing the cost of healthcare through greater use of computer-based patient records systems] to get bogged down in a shouting contest among the players and participants. Each must try to recognize and work together in seeking OPTIMIZATION all sides have to be open to the needs of our society and our technological capabilities in addressing these needs effectively and cost-efficiently."

Robert B. Burleigh, President of Brandywine Healthcare Services and Consultant to the Board of Directors of the International Billing Association (IBA), the only trade association representing third party medical billing companies, also testified before the National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentialityon February 3. 1997. *In his testimony, Mr. Burleigh addressed* various provisions of H.R. 51, proposed legislation to create nationally uniform standards for the confidentiality of health information to assure the safety of the shared information.

In his remarks with respect to Subtitle B - Use and Disclosure of Protected Health Information - Section 111(d), Mr. Burleigh stated: "This section provides that a 'health information trustee may disclose protected health information only if the recipient has been notified that the information is protected health information....' In the normal course of business today, *the technical means of notifying a recipient of (proposed) protected health information, prior to, or concurrently with, disclosure does not exist*. In practice, it would be necessary to identify, with specificity, the information subject

to protection, since some information may be protected in some, but not all instances." Accordingly, he recommended that the "section should be revised to conform with the reality of the flow of medical records information."

In his remarks with regard to Section 112. Authorizations for Disclosure of Protected Health Information, Mr. Burleigh added: "We are concerned that the legislation proposes eight separate elements before a disclosure can be made. In the ordinary course of business, many forms are used to accomplish the same function for multiple providers, particularly in a hospital-based setting. In addition, identification of the payer(s) to receive the information, and the information they will require (the subject of the consent) at the time of consent (crucial to informed consent) is often not possible. The remedy would be both inconvenient and intrusive to the patient and the provider(s)."

And he concluded with the following warning: "We are concerned that an unintended result of this proposed legislation would be the decision by providers to discontinue accepting insurance coverage in order to avoid the burdensome (in their view) new duties of securing informed consents, providing disclosures, maintaining new disclosure logs and related records, and other proposed responsibilities."

On February 4, 1997, Robert Thompson, Vice President of Pharmacy Operations for Revco Drug Stores, testified as a representative of his organization, which operates 2,500 pharmacies in 17 states, and an example of the community pharmacy infrastructure which extends beyond 54,000 retail pharmacies, providing over 60% of the 2.4 billion out-patient prescriptions dispensed annually.

During his testimony, Mr. Thompson states that although his organization "fully supports the intent of federal standards to preserve the confidentiality of patient-identifiable health care information . . . [w]e urge you to consider the real-time impact of requiring patient authorization for the disclosure of patient identifiable information."

Whereas the Total Access design will permit each record repository to set its own standards in accordance with local law, Mr. Thompson shows that this flexibility is not present, nor contemplated, in any of the system designs he is aware of when he stated: "Without total preemption [of state confidentiality laws by federal law], *we will find it impossible to integrate the necessary patient information and authorizations in our computer software. Electronic transmission will become ineffective*."

He concludes by saying: "We believe that the effective date of any legislation should reflect the uncertainty of the unknown costs and technology needed to implement a new federal law. Adequate time must be allowed for software manufacturers to develop their products, to test and distribute the product, and to train [personnel to use them]." Whereas the estimated time to write the Allcare Total Access system is less than 6 months, he asks for 24 months to accomplish this.

FROM TESTIMONY BEFORETHE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, SUBCOMMITTEE ON PRIVACY AND CONFIDENTIALITY
(February 18-19, 1997)

On February 18, Lauren Dame, staff attorney at Public Citizen's Health Research Group, a non-profit organization founded in 1971 by Ralph Nader and Dr. Sidney Wolfe, testified before the committee. *In her prepared remarks, Ms. Dame stated:* "As medical records are computerized and there is increased disclosure of sensitive medical information -- as we believe there will be -- many of the problems consumers face today will be exacerbated unless strong privacy protections are included in any regulations developed. . . . [P]rivacy for medical information is an important value in and of itself. People feel very strongly that they should have control over the dissemination of what amounts to highly intimate and private information about themselves.

"[W]e believe that any effort to regulate the use and development of computerized patient medical records should begin with the proposition that . . . personally identifiable patient information should not be disclosed without the informed consent of the patient. (And, by "informed consent", I do not mean the kinds of blanket consent or release forms patients currently are forced to sign in order to obtain health insurance, which basically give the insurers the right to collect any medical information they want, and to do with it what they will.)"

Ms. Dame concluded her remarks with this statement which indicates the solutions have yet to be devised: "[Y]ou have heard from insurers, providers, and processors of data, and no doubt most of them have painted glowing pictures of the great increases in efficiency and cost savings associated with computerizing medical records and with limiting privacy protections. While in some areas, the interests of all of us might be accommodated, often you will be faced with some hard choices.

"In making your recommendations to the Secretary, I urge you to err on the side of protecting the privacy and confidentiality of personally-identifiable medical information. As a society, we can always modify regulations to increase data exchange *if experience shows us that we can safely do so*. But privacy, once lost, cannot be recaptured."

On February 19, 1997, Dr. Denise Nagel, a physician, instructor at Harvard Medical School and co-founder of the National Coalition for Patient Rights, an organization whose mission is to protect and preserve privacy and confidentiality in medical care, testifyied for that organization and on behalf of the American Psychoanalytic Association and the Association of American Physicians and Surgeons. *During her testimony, Dr. Nagel quoted* the 1996 Time/CNN poll which "found that 87% of Americans believed that 'laws should be passed that prohibit health care organizations from giving out medical information without first obtaining the patient's permission.'" and commented that "the same percentage of people in a 1993 Louis Harris poll trusted their own providers but most (71%) believed that 'if privacy is to be preserved, the use of computers must be sharply restricted in the future.'" Dr. Nagel stated her opinon: "Rules that conform to these views would require consent for placing personal information in a computer system and consent for the disclosure of identified information, except in rare circumstances."

She concluded her remarks with the following statement: "The organizations that I

represent do not have all the answers, but we have a principled approach grounded in the legal, ethical and medical history of our country." It is reasonable to assume that were Dr. Nagel aware of the functionality within the Total Access system, she would have had a solution to offer that would be consistent with her principle-based concerns.

Such an approach would fulfill her concluding comments, made in response to a question from the Committeee chairperson: "The need to protect, preserve *and in some instances restore, the right to medical privacy* in order to preserve quality medical care could hardly be more widely recognized. This Committee has the opportunity to enhance the quality of health care by recommending privacy standards which are consistent with the right to privacy recognized under the Constitution, statutory law, and hundreds of years of medical ethics. Alternatively, this Committee can perpetuate *the current chaotic conditions that are eroding the essential bond of trust between the patient and the treating physician*. We ask the Committee to advance the cause of quality health care, not retard it.

On February 14, 1997, Patrick E. McFarland, the Inspector General of the Office of Personnel Management, the federal agency that oversees the Federal Employees Health Benefits Program (FEHBP), the third-largest health care expenditure program for the United States, testified before the subcommittee. This letter was entered into the record following the subcommittee's February 19, 1997 session. *In his written statement, Mr. McFarland testified*: "Although it is usually not necessary to examine patient treatment records, the additional information obtained through these law enforcement tools are an integral part of analyzing and building a successful case. We must use patient records to determine whether there is a fraudulent pattern of billing or use of patients in schemes to obtain benefits for unnecessary services. My office recognizes the concerns of the public with respect to confidentiality of medical records and mandates a policy to limit our requests to only information necessary for the investigation. *We consider all legal safeguards before disclosing any medical information* to other federal agencies or other individuals.

"With these procedures in place, *any increased restrictions such as a probable cause and notice requirement* for subpoenas contained in recent legislative proposals including HR. 52, The Fair Health Information Practices Act of 1997, *would create what I believe to be an unnecessary and insurmountable burden* on this Office of Inspector General. With a limited staff, adding additional hurdles beyond the present standard of relevancy to the process for accessing medical information would increase the likelihood of litigation at an early investigative stage and would therefore considerably limit the ability to effectively and efficiently investigate, prosecute and deter health care fraud."

OIPE JC189
JUN 0 8 2001
PATENT & TRADEMARK OFFICE

APPENDIX C

ARTICLES EVIDENCING LONG FELT UNMET NEED

ITEM 2

ONLINE HEALTHCARE GETS CANDID ASSESSMENT AT BERKELEY SUMMIT

OIPE JC189 JUN 08 2001 PATENT & TRADEMARK OFFICE

Andrew Hassell

From: "Robert H. Shelton" <RbtShelton@worldnet.att.net>
To: "Andrew M Hassell" <ahassell@prodigy.net>
Cc: "Halden Conner" <hconner1@aol.com>; "John Sigalos" <jlsig1@airmail.net>
Sent: Thursday, June 29, 2000 4:44 PM
Subject: Berkeley Summit Points to Privacy as Critical Issue

See attached article expressing challenges with privacy of individual medical records, and how important a solution to the issue is to the whole industry's future.

I continue to feel that our pending "Private Access" patent application addresses this impediment extremely well. I'm wondering whether we should be providing this kind of article to the USPTO to emphasize that the problem we described in the application is still very much present.

Also, it sure seems like a long time has transpired since we filed that application, with no reply. Should we be checking on its status, if for no other reason than just to make certain nothings been lost in transit...?

<< ONLINE HEALTHCARE GETS CANDID ASSESSMENT AT BERKELEY SUMMIT

Online healthcare has a long, but promising, road ahead of it, according to some scientists and venture capitalists assessing the state of e-health. At the International Biotech and Infotech Summit in Berkeley this week, attendees said that while the Internet is currently changing science, there is still concern that profitable business models are rare in the world of e-health. Summit participants concluded that Web-based medical records, insurance claims, and prescriptions will eventually succeed, but existing technology can't currently handle the data. Additionally, privacy standards and uniform applications need to be in place before both physicians and patients feel confident in e-healthcare.

View full text: http://www.epharm 5.com/news.asp?an=APRS0017939018 >>

<< Online health care, which right now is largely limited to informational and pharmacy Web sites such as PlanetRx.com and WebMD.com, has been hyped a great deal. But profitable business models - and reasons for investing - are few and far between, Colella said.

To be sure, the Internet could streamline medical records, insurance claims and prescriptions, but the computing power needed to handle all that data is several years away, panelists said. And until better technology and viable business models come along, investing in e-health care is "still an incredibly high risk," Colella said.

Thus far the only profits associated with online health care have come from business-to-business transactions such as medical supply auctions, and from shepherding online "communities" of patients toward products that interest them, panelists said.

But the roadblocks to the one-click health care system of the future are not just about business models and technology. Medical records are another frontier.

Putting records online would make it possible for any doctor anywhere to see a patient's comprehensive medical history, thus avoiding duplicate tests and making it far easier to diagnose illness.

But Americans are still not comfortable enough with security on the Web to put their records online, said Dr. Mark McClellan, an assistant professor at Stanford University's Center for Health Policy.

"There's still a fundamental perception problem of whether people think medical records online are safe," McClellan said. "Most Americans do not think so."

Providing such widespread access to medical histories also raises ethical questions, McClellan said....

The fear is that if medical records or genetic information about individual humans gets into the wrong hands - particularly if it happens long before cures are developed - discrimination could result.

Complicating matters further, there is no standard medical-record format that every hospital, insurance provider and doctor uses, McClellan said. All these health care entities would have to agree on a format before the information could be put online with any efficiency, he said.

Despite the obstacles, the experts at Tuesday's conference, entitled "Into the 21st Century: Genomics and Beyond," were still enthusiastic about online health care's potential.

"E-health care is one of the few things in the last 50 years that could improve not only the quality of health care but its efficiency," said Laura D'Andrea Tyson, dean of UC Berkeley's Haas School of Business. >>

OIPE JC103
JUN 0 8 2001
PATENT & TRADEMARK OFFICE

APPENDIX C

ARTICLES EVIDENCING LONG FELT UNMET NEED

ITEM 3

PRIVACY TECHNOLOGY STILL MISSING THE MARK

OIPE JC16 JUN 0 8 200 PATENT & TRADEMARK OFFICE

Andrew Hassell

From: "Robert H. Shelton" <RbtShelton@worldnet.att.net>
To: "Andrew M Hassell" <ahassell@prodigy.net>; "John Sigalos" <jlsig1@airmail.net>
Sent: Thursday, July 06, 2000 3:29 PM
Subject: Privacy Technology Still Missing the Mark

Timely article that appeared in today's trade publication for ePharmaceuticals....

<< 5. PRIVACY TECHNOLOGY STILL MISSING THE MARK

A recent effort to improve online privacy by customizing Web browsers still has loopholes, according to an article in the San Francisco Chronicle. P3P, an emerging technology being developed by the World Wide Web Consortium, allows Internet users to specify what type of information a website can collect from them. Both Microsoft and Netscape are planning to install P3P technology in their next browser upgrades. The downside, according to the Chronicle, is that many sites may not choose to implement P3P. In addition, the software still doesn't control how websites use information that is collected with the users' permission.

http://www.epharm5.com/news.asp?an=SFC0018500452 >>

Here's what the summary referred to...

<< P3P Needs To Be Better At Privacy

Henry Norr
The San Francisco Chronicle

From Bill Clinton to Bill Gates, the establishment is rallying around a new Internet standard called P3P. It's an interesting development, but watch out for the hype they're spinning about it.

Although P3P (which stands for Platform for Privacy Preferences) is still just a working draft -- even after more than three years of development -- the White House, AOL, AT&T, Hewlett-Packard, IBM and even Procter & Gamble have already implemented it on their Web sites. Microsoft and Netscape plan to build support for it into the next release of their respective browsers.

According to the World Wide Web Consortium, the nonprofit but industry-dominated body sponsoring the standard's development, its purpose is to provide "a simple, automated way for users to gain more control over the use of personal information on Web sites they visit."

To judge by the spec and accompanying documentation at the P3P home page (www.w3.org/P3P), it will probably live up to that claim -- in a way. Its purpose is to define a standard, machine-readable language for describing privacy policies -- what kind of personal information a Web site proposes to collect from users and how it intends to use the data.

This turns out to require a surprisingly complex vocabulary. In addition to terms for many kinds of demographic information -- birth date, gender, home address and so on -- it also covers several types of dynamic data, such as the "referrer" (the site the user came from), the "clickstream" (exactly what the user clicks on while visiting a site) and what he or she may have searched for.

That's the easy part, though. The real challenge was to reduce the variety of ways a site might use such information to a handful of variables -- for example, how long the site will retain the information it collects, whether it will use the data to contact the individual to promote a product or service, whether it will compile data into profiles of user habits, whether such profiles will be anonymous or linked to personal identifying information, etc.

On the user side, a P3P-enabled browser would store the user's preferences about such matters, then compare those preferences to the policies of sites he or she visits. When the user -- call her Sally Surfer -- goes to a site whose policies match her preferences, she could cruise through it just as she does today, except that her browser might display an icon indicating that everything is hunky-dory from a privacy perspective.

Exactly what happens when Sally hits a site whose policies don't correspond to her preferences isn't defined in the current P3P spec; that's left up to the developer of the browser or other P3P- compliant software she's using.

Most likely, though, the program would put up a dialog box alerting Sally to the discrepancy and giving her a choice between accepting the site's policies or giving up her plan to visit it. Earlier drafts of the specification included a scheme for electronic haggling over such matters -- a way for users to get more benefits for providing more information -- as well as a mechanism for automatically transmitting personal data authorized by the user's preferences.

Those provisions, however, have been dropped -- the first because of its technical complexity, the second reportedly because polling showed widespread user resistance to background transfer of their personal information.

What's left is pretty modest, considering how long the standard has been in gestation and how many powerful players have been involved. As far as it goes, it strikes me as a modest step in the right direction.

But it's also a far cry from what we so obviously need: clear and enforceable rules about the collection and use of personal information. Consider:

-- Web site operators won't be under any obligation to implement P3P. Lots of them -- the sleazy, the lazy, those who lack the technical skills or software required -- will undoubtedly just ignore it. And it certainly doesn't address the problem of the failed dot- coms, which, as Cnet reported last week, are cheerfully auctioning off information about their former customers, possibly including phone and credit-card numbers, home addresses and purchase histories (news.cnet.com/news/0-1007-200-2176430.html?tag=st.ne.1002.tgif.ni)

-- Even if they're machine-readable, privacy policies are inevitably complex, so I suspect most users won't bother to configure the software for their own considered preferences -- they'll just accept the default settings.

-- Nothing in the standard says what those defaults should be. Because no user wants to be turned away from a site she's already navigated to, and most will find it burdensome and confusing to have to reconfigure their preferences before they can get where they're going, browsermakers will be under pressure from users as well as site operators to keep the bar low. (Don't forget: These are the same browsermakers who brought us the cookie -- and have since provided only the crudest tools for controlling this frightful mechanism.)

-- Neither technical standard can guarantee that sites actually do what they say they will, whether they state their policies in bits and bytes or in B2C bureaucratese. Nor can a standard impose any penalty on those who violate their commitments.

-- By accepting and formalizing the idea of trading personal data for access, P3P could have the effect of encouraging sites that don't collect such data to start doing so.

Despite all these shortcomings, many proponents of P3P are using it to justify their opposition to more meaningful solutions to the Internet privacy, such as laws of the sort that just about every other developed country already has -- and that we in the United States have enacted to protect other kinds of personal information, including telephone and video-rental records.

It's no wonder, then, that many seasoned privacy advocates are leery of P3P. The Electronic Privacy Information Center, a Washington, D.C., public-interest group that's been working on the issue for six years, and Junkbusters, an organization run by a computer scientist with a doctorate in data mining, have just issued a scathing critique under the title "Pretty Poor Privacy"

(www.epic.org/reports/prettypoorprivacy.html).

And even groups that support P3P acknowledge its limitations -- see, for example, the assessment produced by the Center for Democracy and Technology in cooperation with the office of Ontario's Information and Privacy Commissioner, which is posted at www.cdt.org/privacy/pet/p3pprivacy.shtml.
Something here.

NIXON TO THE RESCUE? One irony about the sad state of privacy protection in the United States: This country isn't just the home of the Bill of Rights and what Justice Louis Brandeis called "the right to be let alone" -- it's also the home of the principles on which Europe's computer-era privacy regulations are based. Known as the Code of Fair Information Practices, these guidelines were developed by a commission set up by, would you believe, the Nixon administration. (I owe that tidbit to "Database Nation," Simson Garfinkel's excellent new book on the privacy problem, published by O'Reilly.)

Here are the five key principles of the code, as articulated (according to Garfinkel) in a 1973 report of the then Department of Health, Education and Welfare:

-- There must be no personal data record-keeping system whose very existence is secret.

-- There must be a way for a person to find out what information about the person is in a record and how it is used.

-- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

-- There must be a way for a person to correct or amend a record of identifiable information about the person.

-- Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Giving these principles the force of law is no privacy panacea -- there isn't one -- but at least it would get at the heart of the problem, which is more than one can say about P3P. >>

OIPE JC189 JUN 08 2001 PATENT & TRADEMARK OFFICE

2772
2671 AF

ANDREW M. HASSELL
Attorney at Law
12568 Burninglog Lane
Dallas, Texas 75243-3230
972-234-6540

June 6, 2001

RECEIVED
JUN 13 2001
Technology Center 2600

Honorable Commissioner Patents & Trademarks
Washington, D. C. 20231

Re: Patent Application of ROBERT H. SHELTON
Serial No. 09/025,279
Filed: February 17, 1997
For: STANDING ORDER DATABASE SEARCH SYSTEM AND METHOD FOR INTRANET AND INTERNET APPLICATION
Group Art Unit 2172
Examiner: Jean B. Fleurantin

Sir:

Please find enclosed the following documents relating to the above-identified matter:

Appeal Brief in Triplicate (including Appendices A, B and C)
Check in the amount of $310.00 for the required fee
Self-addressed postal card for acknowledging receipt of the foregoing

Thank you for your attention to this matter.

Respectfully,

Andrew M. Hassell

Andrew M. Hassell
Registration No. 18182
Attorney for Appellant
12568 Burninglog Lane
Dallas, Texas 75243
Tel: (972) 234-6540
Fax: (972) 234-6540

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.